



Qualys Security Conference Mumbai, India

Qualys Container Security

Comprehensive Security for the ever-changing Container Stack

Hari Srinivasan

Director Product Management, Qualys, Inc.



Everybody Loves Containers



Portability

Agility

Density

Container Components & Lifecycle

Docker File

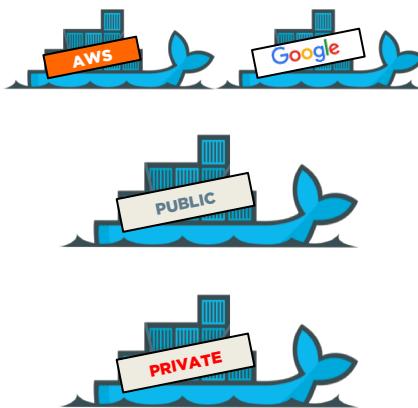
```
#Apace Image  
FROM Ubuntu:12.04  
RUN apt-get update  
RUN apt-get install -y  
apache2  
ENV APACHE_RUN_USER  
www-data
```

Image

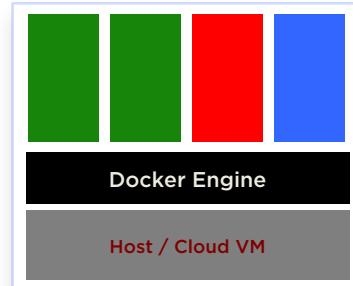


myApache:2.2:Latest

Image Registry



Containers

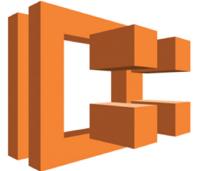


Container Platforms

On Premise



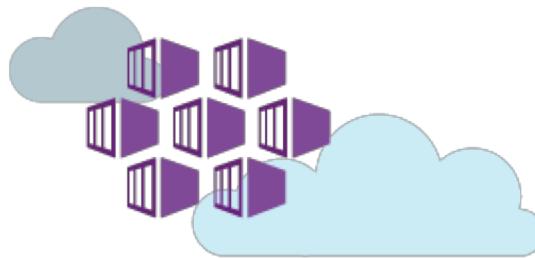
Cloud



Amazon ECS



Amazon EKS



Azure Container Service



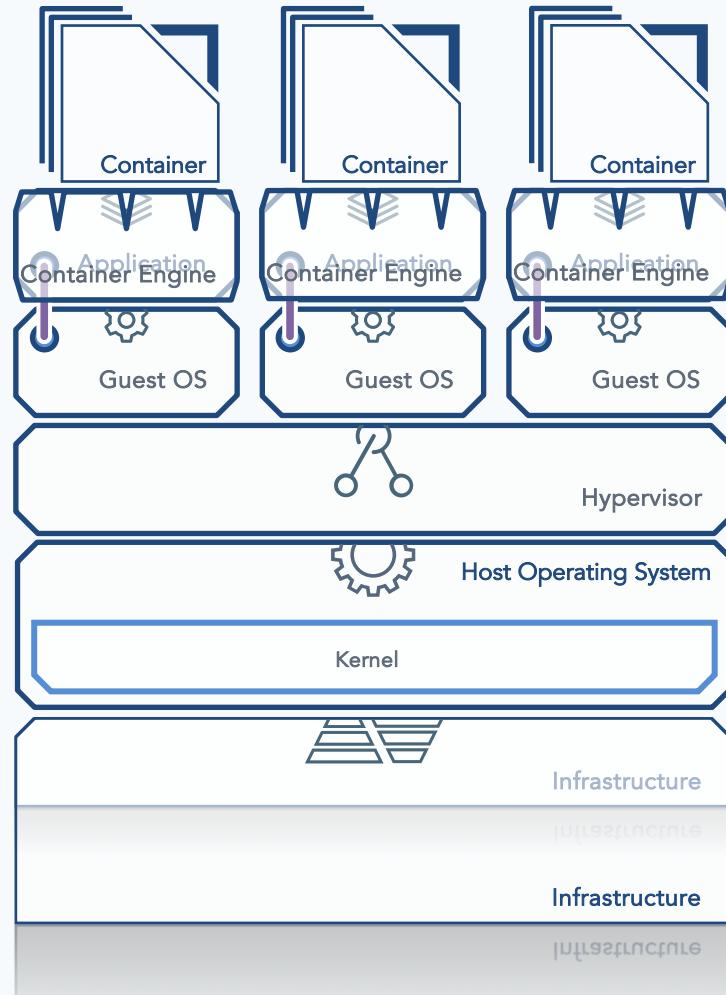
Google Cloud Container Engine

Container Deployments

Deployment Scenario #1

Use Case

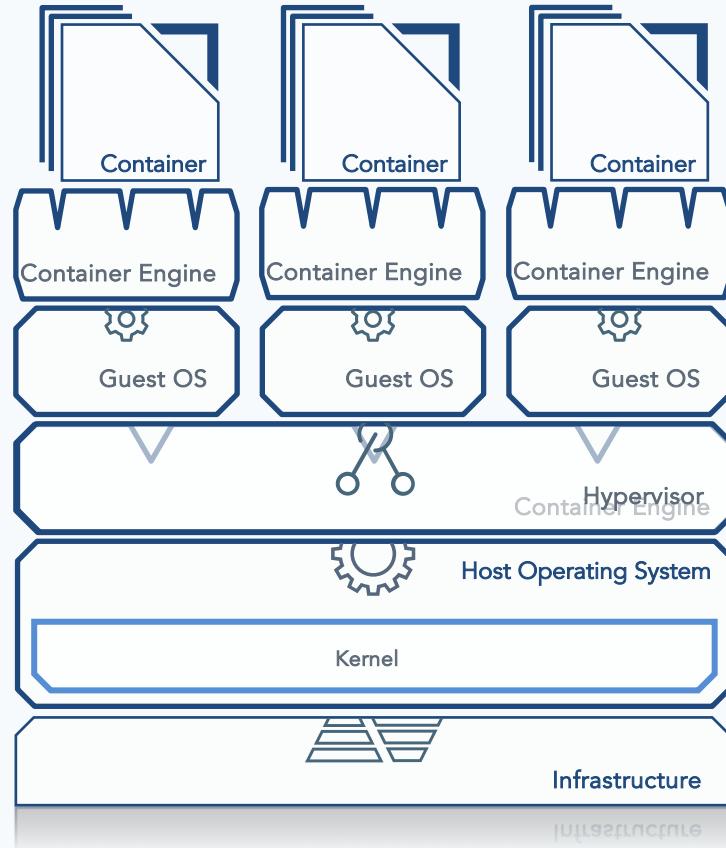
1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines



Deployment Scenario #2

Use Case

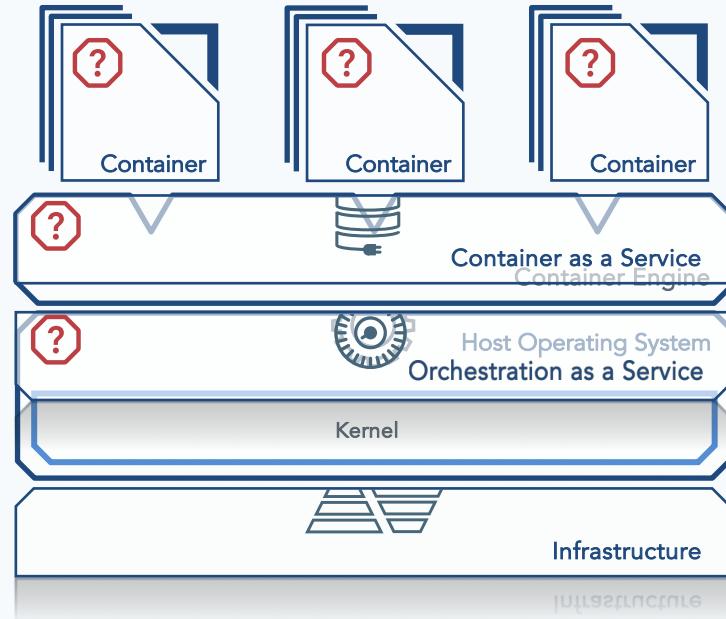
1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters



Deployment Scenario #3

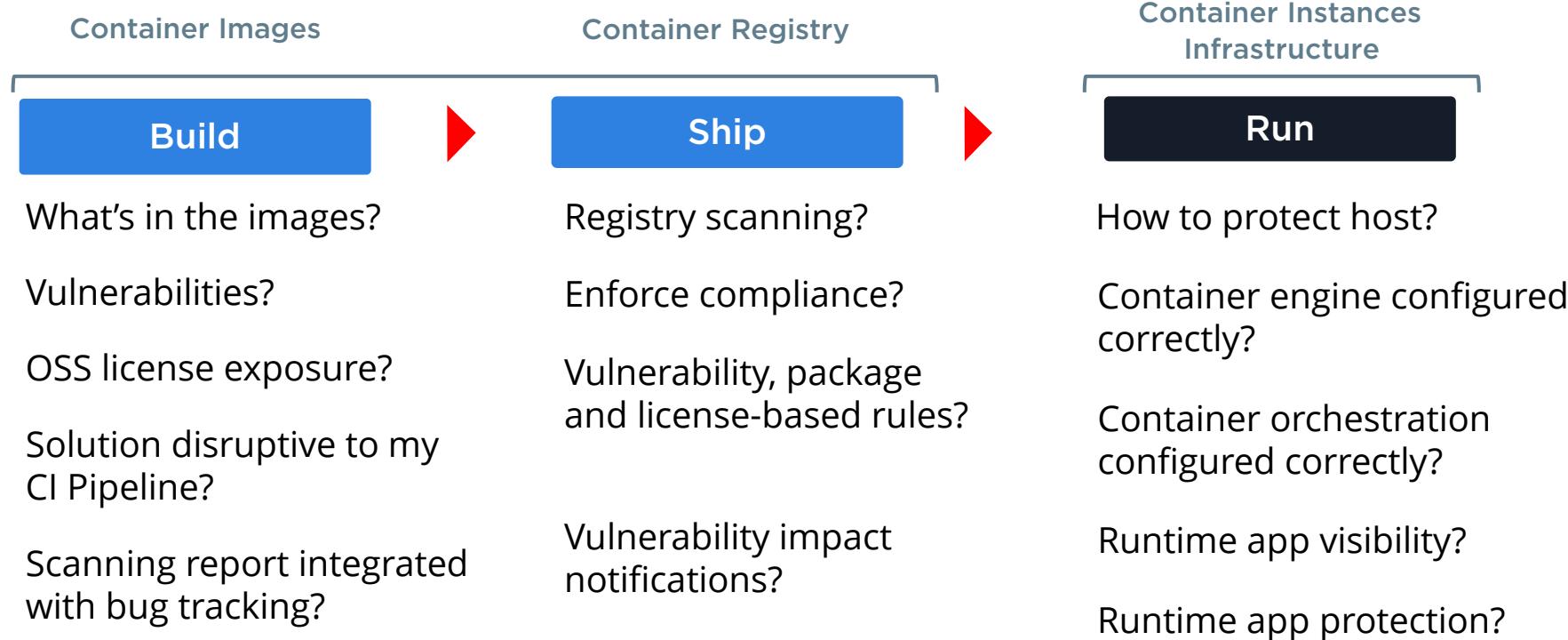
Use Case

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?



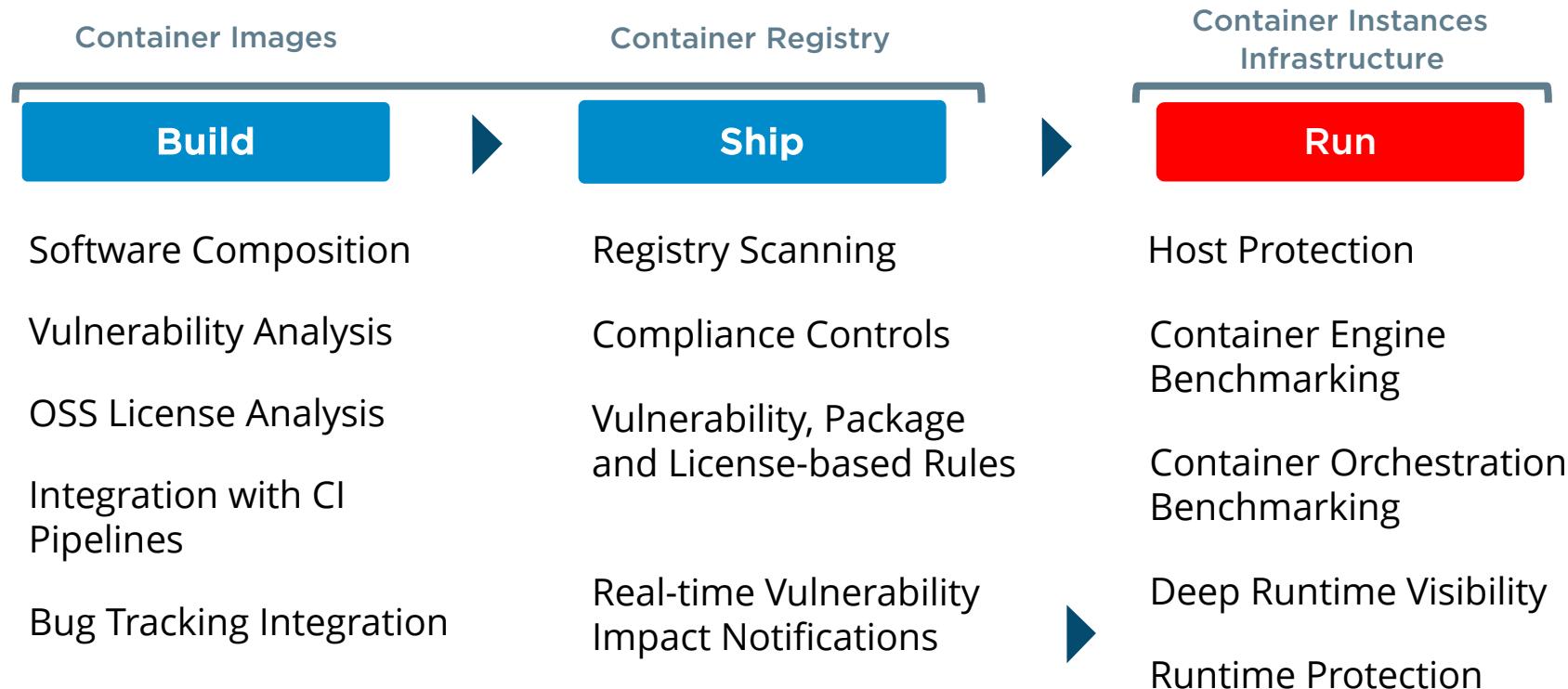
Container Visibility & Security Challenges

Container Lifecycle Challenges



Qualys Container Security

Qualys Container Security



Qualys Container Security

Key Uses



Visibility into your container projects

Identify Hosts with Containers. Inventory of images, containers. Search images with vulnerabilities, labels, tags, packages,.. Build custom widgets.



Secure the CI/CD pipeline

Integrate images, vulnerability scans into the build. FAIL builds, not allowing unsecure images to enter the stream



Scan Registry and block unauthorized images

Inventory and scan as new images are added to the registry. Block unapproved images from being spun up as Containers.



Container Runtime Visibility and Protection

Find what containers are running, know if the runtime got changed from images. Protect from changes or breakouts.

Use Case #1

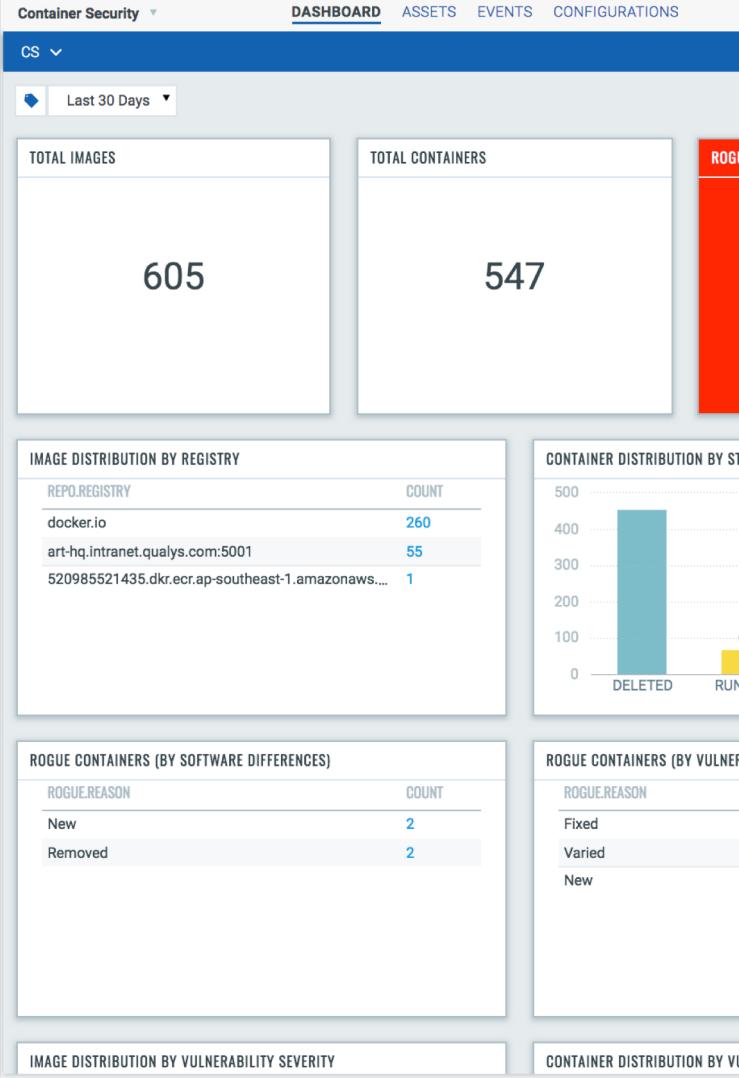
Visibility into your container projects

Overview Dashboard

Inventory & security posture widgets

- Container Hosts
- Count of images, containers
- Containers by state
- Vulnerable images

Personalize and add custom widgets



Know where your Containers are?

- Inventory of all Container Hosts across your datacenters, public clouds, laptops,..
- Know how the host vulnerabilities, exploits affect your container environments

Qualys Enterprise AssetView

Dashboard Assets Templates Connectors

Docker Container Hosts Visibility

Actions Add Widget

DOCKER EASYEXPLOIT & PATCHABLE PER SEVERITY

Severity	Count
3	6
4	1

DOCKER HOSTS

10

DOCKER HOSTS BY ALL CLOUD PROVIDERS

Name	Operating System	Count
AWS	Amazon Linux	4
AWS	Amazon Linux 2018.03	3
GCP	Ubuntu Linux 16.04.6	3

CONTAINERS 1-10

CONTAINERS 11-20

CONTAINERS 21-30

DOCKER HOSTS

Name

Host Scan Time

Contents of /etc/iss

Linux Kernel Versi

Contents of rsyslog

"daemon.notice" E

Installed Packages

Netstat - Unix Conn

Internet Protocol v4

Know where your Containers are?

The screenshot shows the AssetView interface with two separate search results. The top search result is for assets where `isDockerHost: "true"`. The bottom search result is for assets where `operatingSystem: mac` and `software.name: docker`.

Top Search Result (isDockerHost: "true"):

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
qcs-g-01	Ubuntu Linux 16.04.6 fe80:0:0:506d:7eff:fc1:9bc9, ...	VM PC	amandern	Inventory Scan Complete an hour ago	Cloud Agent	
qcs-r-1	Ubuntu Linux 16.04.6 172.17.0.1, 10.138.0.3, fe80:0:0:...					
qcs-g2	Ubuntu Linux 16.04.6 172.17.0.1, fe80:0:0:4001:aff:fe...					

Bottom Search Result (operatingSystem: mac and software.name: docker):

Asset Name	OS	Modules	Last Logged-In User	Activity
10235mbp15.local	Mac OS X 10.13.6 10.0.1.105, fe80:0:0:0:1447:8717...	VM PC	mquealy	Scan Complete 11 hours ago
101298mbp15.local	Mac OS X 10.13.6 172.20.0.95 101298mbp15	VM	mwalker	Scan Complete 13 hours ago

Annotations:

- A red circle highlights the first asset in the top search result (qcs-g-01).
- A red circle highlights the first asset in the bottom search result (10235mbp15.local).
- A red arrow points from the text "Servers - Datacenter, Clouds, etc.." to the first red circle.
- A red arrow points from the text "Developer Mac laptops" to the second red circle.
- Text at the bottom left: "isDockerHost: "true" and provider: AWS/Azure/GCP"

Image Inventory and Smart Searches

The screenshot shows the Qualys Container Security interface. On the left, there's a sidebar with 'Assets' statistics (68 Total Images), 'LABELS' (NGINX Docker M...), 'REGISTRY' (Docker.io 68, Art-Hq.Intranet.Q... 1), and 'VULNERABILITIES' (Severity 5 68, Severity 4 65, Severity 3 59). The main area has tabs for 'DASHBOARD', 'ASSETS' (selected), 'EVENTS', and 'CONFIGURATIONS'. A search bar at the top right contains the query: 'vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"'. Below the search bar is a table titled '1 - 50 of 68' showing image details:

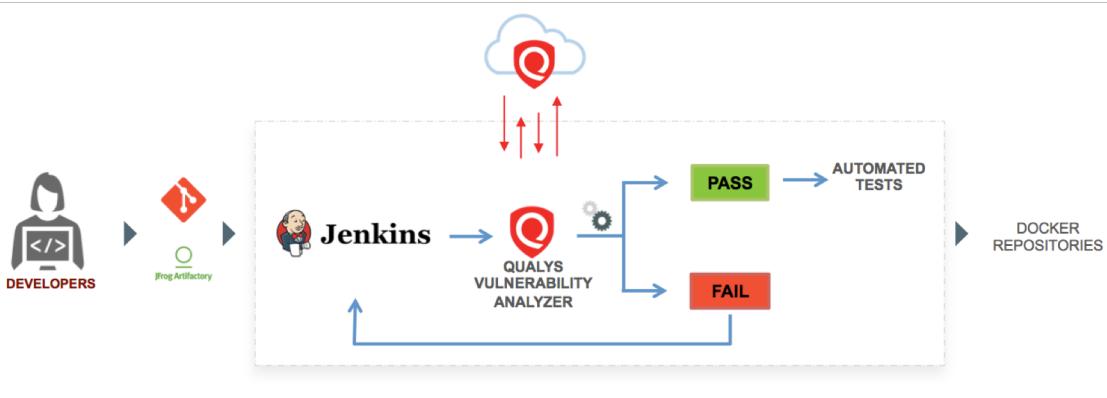
REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch	Feb 06, 2018	latest	0 On Hosts: 1	2
docker.io	redis	Feb 06, 2018	latest	1 On Hosts: 1	3
docker.io	kibana	Feb 06, 2018	latest	0 On Hosts: 1	3
docker.io	node	Feb 01, 2018	latest	0 On Hosts: 1	3
docker.io	httpd	Jan 26, 2018	latest	1 On Hosts: 1	3
docker.io	cassandra	Jan 23, 2018	latest	0 On Hosts: 1	4
docker.io	solr	Jan 19, 2018	latest	0 On Hosts: 2	14
docker.io	tomcat	Jan 18, 2018	latest	0 On Hosts: 1	13
docker.io	kibana	Jan 17, 2018	latest	0 On Hosts: 1	10

Annotations on the left side highlight features: 'Search based on all attributes' points to the search bar, and 'Preset quick search filters - Identify images by application labels' points to the 'LABELS' section. Annotations on the right side highlight features: 'Image info', 'Registry info', 'Containers for this image', 'Vulnerability posture?', and 'Easy drill down for complete inventory' point to various parts of the interface.

Use Case #2

Secure the CI/CD pipeline

Block vulnerable images
in the build



Download the Qualys Vulnerability Analysis plug-in for Jenkins and install on the Jenkins master

Install the Qualys Container Sensor on the Jenkins worker nodes

Set up policies to Pass/Fail the build. Ex: No Sev.5 vulnerabilities, > CVSS 7, specific QID, vulnerabilities count. Etc.

Plugins:



REST APIs for any other integrations.

*TeamCity, CircleCI - Support coming soon

Actionable Vulnerability Information

Jenkins > pipeline-project > #78 > Qualys Report For e8d112ff7588

3 search ?

BUILD REPORT - e8d112ff7588

Build Status: Failed Image ID: e8d112ff7588
Tags: latest Size: 828 MB

Build Summary

The vulnerabilities count by severity for image id e8d112ff7588 exceeded one of the configured threshold value :
Configured : Severity 1 > 0; Severity 2 > 0; Severity 3 > 0; Severity 4 > 0; Severity 5 > 0;
Found : Severity 1: 0, Severity 2: 1, Severity 3: 11, Severity 4: 2, Severity 5: 0

Vulnerabilities Trend

Severity	Count
Sev 5	0
Sev 4	1
Sev 3	11
Sev 2	2
Sev 1	0

Confirmed Vulnerabilities (10)

Severity	Count
Sev 5	0
Sev 4	1
Sev 3	9
Sev 2	0
Sev 1	0

Potential Vulnerabilities (4)

Severity	Count
Sev 5	0
Sev 4	1
Sev 3	2
Sev 2	1
Sev 1	0

Patchability

Status	Count
Yes (12)	12
No (2)	2

Qualys Report For e8d112ff7588

INSTALLED SOFTWARE

Show 10 entries Search: QID=176259

Name	Installed Version	Fixed In Version
libmagickwand-dev	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4

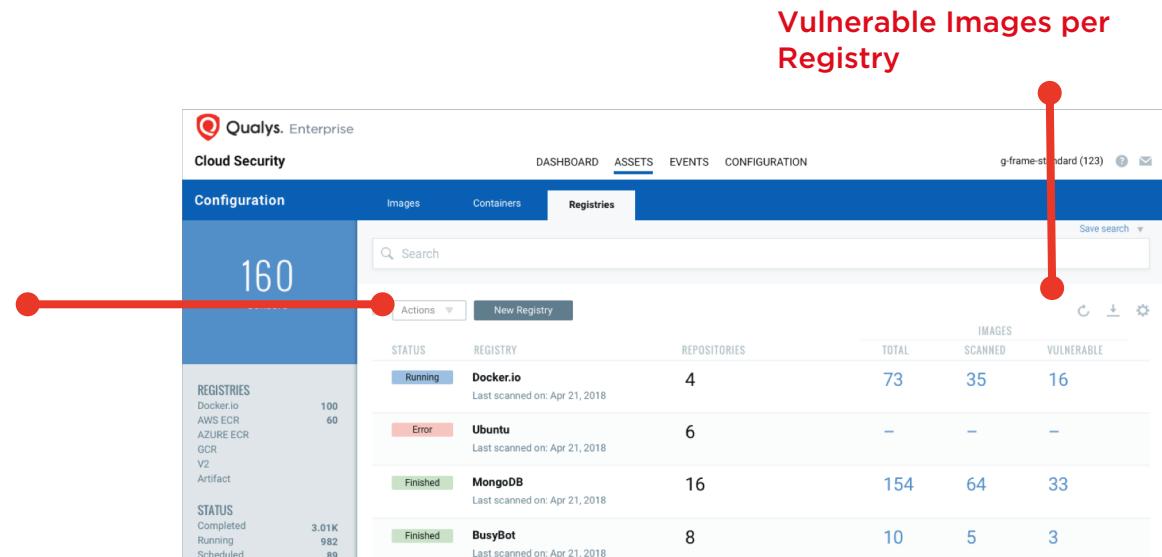


Use Case #3

Scan Registry and block unauthorized images

Detect threats from images being shipped

Know your Registries



Inventory Registry

Qualys. Enterprise

Cloud Security

DASHBOARD ASSETS EVENTS CONFIGURATION g-frame-standard (123) ? ⚡

Configuration Images Containers Registries

Save search ▾

160 Sensors

REGISTRIES Docker.io 100 AWS ECR 60 AZURE ECR GCR V2 Artifactory 3.01K 982 89

STATUS Completed 3.01K Running 982 Scheduled 89

Search

Actions New Registry

STATUS	REGISTRY	REPOSITORIES	TOTAL	SCANNED	VULNERABLE
Running	Docker.io	4	73	35	16
Error	Ubuntu	6	-	-	-
Finished	MongoDB	16	154	64	33
Finished	BusyBot	8	10	5	3
Running	waf-appliance	22	22	9	7
Running	oraclelinux	3	6	6	1

Qualys. Enterprise

Create New: Registry

← STEPS 1 / 2

Registry Information
Name and select the type for this registry. If Public, add credentials if needed.

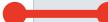
Scan Settings

REGISTRY TYPE:
Select one...
AWS ECR
DockerHub
Artifactory V2
Docker Trusted Registry

Docker V2 Private

PASSWORD:

Cancel Previous Next

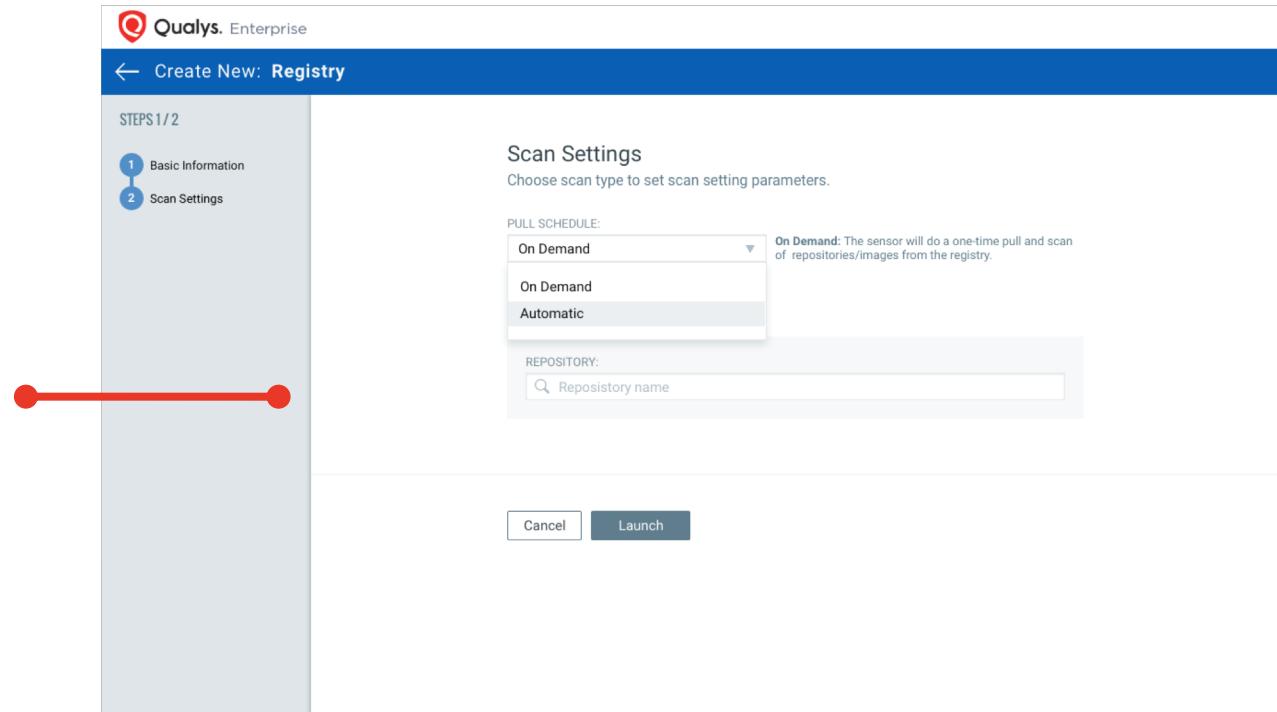


* Support coming soon

Setup Scans

Configure scan frequency
for image vulnerability
analysis

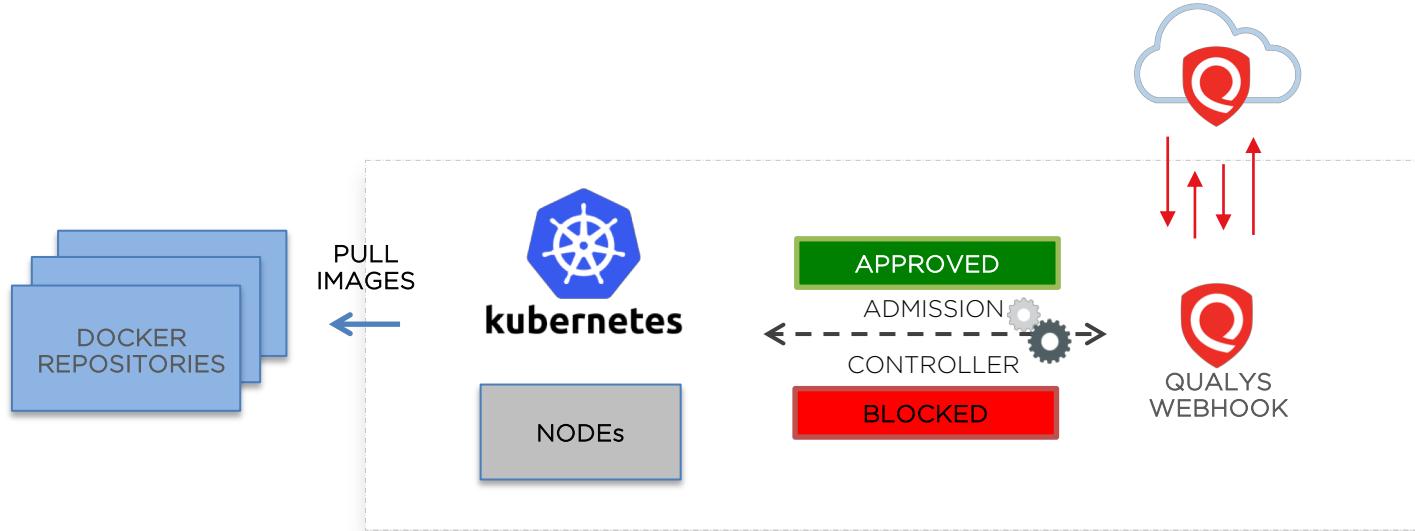
Automate scanning of
images every day at a
scheduled time



* Support coming soon

Policy based Orchestration

Blocking unapproved images spun up as containers





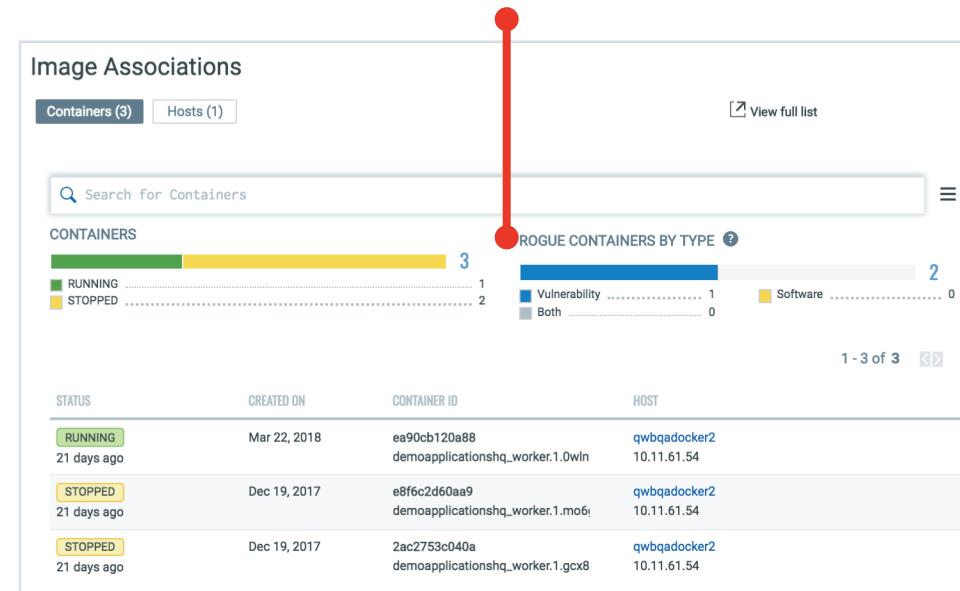
Use Case #4

Runtimes Drifts & Protection

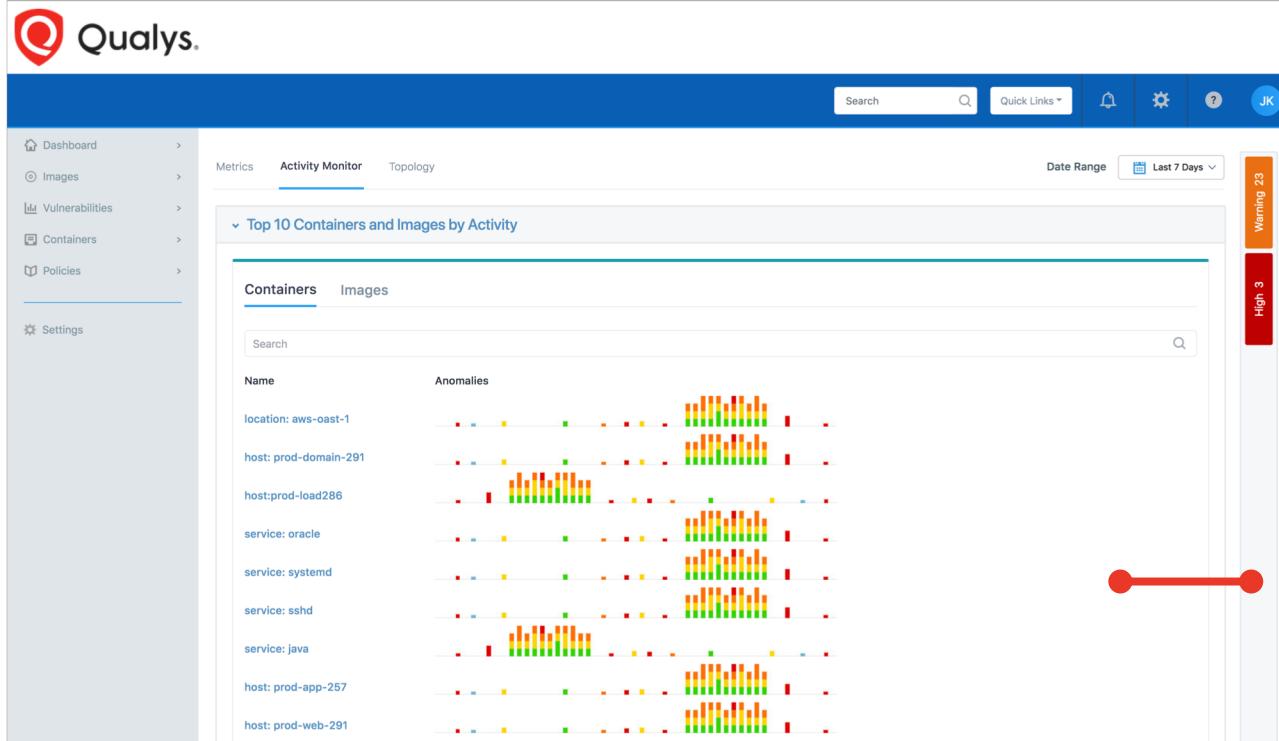
Detect Containers breaking off from “immutable” behavior and Block/Kill/Quarantine them.

Identify potential breaches in containers

“Rogue” Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc



Containers breaking off from the “immutable” behavior



-  Dashboard >
 -  Images >
 -  Vulnerabilities >
 -  Containers >
 -  Policies >
-
-  Settings

Metrics **Activity Monitor** Topology

Date Range

 Last 7 Days 

Container Details



Just now

sys_read



sys_write



sys_open



sys_close



sys_stat



sys_fstat



sys_lstat



sys_writev



sys_pipe

 Warning 23

High 3

-  Dashboard >
-  Images >
-  Vulnerabilities >
-  Containers >
-  Policies >
-  Settings

Metrics **Activity Monitor** Topology

Date Range

 Last 7 Days 

Event Details



Just now

5 minutes ago

Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

Process	Process ID	Call	Arguments	Action	Time
/usr/sbin/httpd	31	sys_execve	/bin/sh	Deny	11/13/2018, 12:48:23AM

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd

Warning 23

High 3

Qualys Container Security

Host Protection

CIS Benchmarks

Protection for container infrastructure stack

Scanning & Compliance

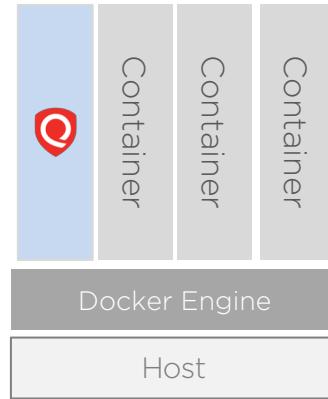
Accurate insight and control of container images

Visibility & Protection

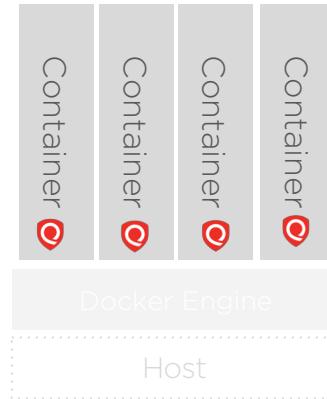
Automated analysis and enforcement of container behavior

Qualys 'Container Security' Sensor Options

Qualys Container Sensor
Side-car*

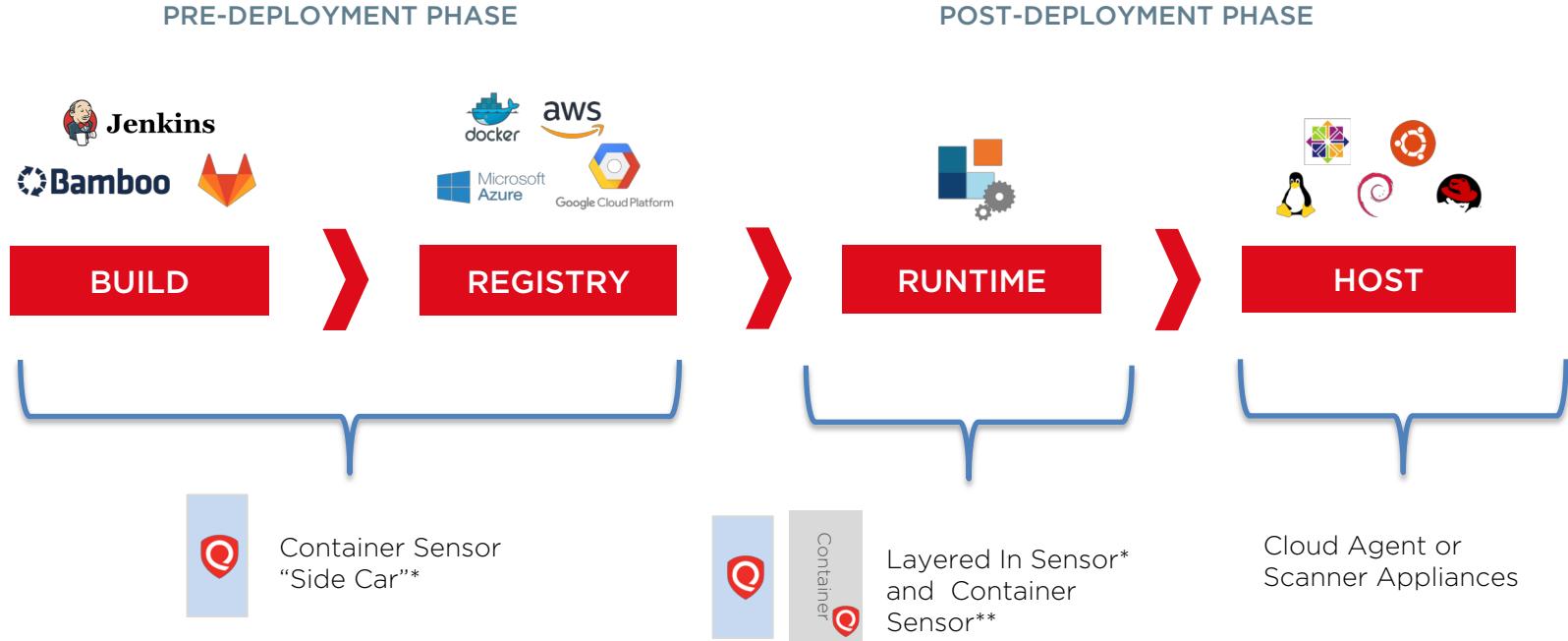


Qualys-Layered Insight
Embedded option



* Qualys side-car to 'all' containers on the node. Runs today as non-privileged.
As features of compliance and enforcements are added the mode will change
to Privileged, with option to revert to non-privileged

Sensors for every use case



* Layered In option for runtime protection

** Prevention from starting off malicious containers



Qualys Security Conference Mumbai, India

Thank You

Hari Srinivasan
hsrinivasan@qualys.com